STATE BANK OF VIETNAM **-------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **---------------**
No.18/2018/TT-NHNN	*Hanoi, August 21, 2018*

CIRCULAR

ON INFORMATION SYSTEM SECURITY IN BANKING OPERATIONS

Pursuant to the Law on the State Bank of Vietnam dated June 16, 2010;

Pursuant to the Law on Credit Institutions dated June 16, 2010 and the Law on amendments to the former Law dated November 20, 2017;

Pursuant to the Law on E-Transaction dated November 29, 2005;

Pursuant to the Law on Information Technology dated June 29, 2006;

Pursuant to the Law on Cyber information security dated November 19, 2015;

Pursuant to Decree No.16/2017/ND-CP dated February 17, 2017 of the Government on functions, duties, rights and organizational structure of the State Bank of Vietnam;

At the request of the Director of Information Technology Authority;

Governor of the State Bank of Vietnam promulgates a Circular on information system security in baking operations.

Chapter I

GENERAL PROVISIONS

Article 1. Scope and regulated entities

1. This Circular provides for assurance of information system security in baking operations.

2. This Circular applies to credit institutions (except for people's credit funds and microcredit institutions), branches of foreign banks and intermediary payment service providers (hereinafter referred to as "institutions").

Article 2. Definition

For the purpose of this Circular, the terms below shall be construed as follows:

1. "information system" means a collection of hardware and software appliance, database and network system used for producing, transmitting, receiving, collecting, storing and exchanging digital information that support one or more than one technical and professional operation of an institution.

2. “confidentiality of information” means assurance that information is only accessible to persons who are granted equivalent permissions.

3. “integrity of information” means assurance that accuracy and sufficiency of information are protected and any change to information is only permitted by authorized persons.

4. “availability of information” means assurance that authorized persons are able to extract information whenever they need.

5. “information security” means protection of digital information and information system from unauthorized access, use, disclosure, interruption, change or illegal disruption with the aim of ensuring the confidentiality, integrity and availability of information.

6. “information technology risk” means probability of loss when carrying out operations relating to information systems. Information technology risk relates to management and use of hardware, software, communication, system interface, operation and people.

7. “cybersecurity incident” means incident in which digital information and information system are attacked or harmed resulting in negative effects on their confidentiality, integrity and availability.

8. "technical vulnerability" means any component of information systems that is highly vulnerable to attack or unauthorized access for use purpose.

9. “data center” includes technical infrastructure (base station and cable system) and computer system with auxiliary equipment installed into such system for the purpose of processing, storing, exchanging and managing data in a concentrated manner.

10. “mobile device" means a digital device which can be hand-held without any effect on its operating capability and has an operating sytem, capability to process or connect to a network as well as a display screen such as a laptop, tablet and smartphone.

11. “information-bearing object" means physical means used for storing, transmitting and receiving digital information.

12. “firewall” means a collection of components or a system of equipment and software that is placed between two networks with the aim of controlling all outgoing and incoming connections.

13. “untrusted network” means an external network connecting to the internal network of an institution which is not under management of such institution or any foreign credit institution in

relation to such institution such as affiliated entity or commercial presence of such institution in Vietnam.

14. “cloud computing service" means offering computing resources through network environment which enables ubiquitous users to access, adjust and pay according to the using requirement.

15. “user account” or "account" means an unique collection of information representative of an user on the information system which is used for logging in and accessing to resources permitted on such information system.

16. “third party” means any individual or enterprise (excluding foreign credit institution and members of the foreign credit institution in case the institution is an affiliated entity or commercial presence in Vietnam of such foreign credit institution) entering into a written agreement (hereinafter referred to as "contract for service use") with the institution to supply information technology services.

17. "competent authority” means a title or person authorized in writing to perform one or more than one duty of an institution by the legal representative of such institution.

Article 3. General principles

1. The institution shall take responsibility to ensure information security under the principle that clearly defines power and responsibility of each department and individual in such institution.

2. Information system shall be categorized in order of importance under an appropriate information security policy.

3. Information technology risks that are probably incurred in the institution must be timely identified, classified, assessed and efficiently handled.

4. Information security regulations shall be established and adopted according to regulations herein and harmony in interests, costs and the ability to take risk of the institution shall be ensured.

Article 4. Classification of information and information system

1. Information processed and stored through the information system shall be classified by confidentiality as follows:

a) Public information refers to information that is publicly disclosed to any person without determination of his/her identity and address;

b) Internal information refers to information of an institution not yet managed and used under authorization given to an identified person or a group of identified persons in such institution;

c) Classified information refers to information that is categorized as (i) confidential information in compliance with the institution's regulations and is only accessed by restricted persons or (ii) third-degree, second-degree and first-degree secret information as per provisions of the Law on Protection of State secrets.

2. Criteria for importance-based classification of information systems of institutions:

a) Normal information system (Level 1) refers to the information system that supports internal operations of an institution or clients services without classified information processing;

b) Important information system (Level 2) refers to one of the following information systems: (i) information system providing classified information processing; (ii) information systems that supports daily internal operations of an institution with no operation termination over 4 working hours; (iii) 24/7 information system for client service with no operation termination without plan in advance; (iv) information system providing online transaction for the clients;

c) Specially important information system (Level 3) refers to one of the following information systems: (i) 24/7 national information system in banking serving development of e-government which allows no operation termination without plan in advance; (ii) 24/7 information infrastructure system for common use in banking that supports operations of agencies and organizations nationwide which allows no operation termination without plan in advance;

d) In case the information system includes more than one component system and each component system is categorized by different importance, such information system shall be categorized by importance of the component system that provides primary technical and professional actitives.

3. Institutions shall classify their information system by importance prescribed in Clause 2 this Article. The list of information system categorized by importance must be approved by the legal representative of such institution.

Article 5. Information security regulations

1. The institution shall set out information security regulations in consistent with its information system, organizational structure, management requirement and operations. Information security regulations must be signed for issuance by the legal representative of such institution and imposed throughout such institution.

2. Information security regulations shall at least contain basic contents as follows:

a) Management of information technology assets;

b) Management of human resources;

c) Assurance of safety in terms of physical and installation environment;

d) Management of information use and exchange;

dd) Access management;

e) Management of use of information technology service provided by a third party;

g) Management of acceptance, development and maintenance of information systems;

h) Management of information security incidents;

i) Assurance of continuous operation of information systems;

k) Internal inspection and reporting mechanism

3. The institution shall carry out review of information security regulations at least once every year and ensure sufficiency of those regulations as per provisions herein. When discovering any shortcoming which causes insecurity of the information system or as required by competent authorities, the institution shall carry out amendment or adjustment to the issued information security regulations.

Chapter II

REGULATIONS ON ASSURANCE OF INFORMATION SECURITY

Section 1. MANAGEMENT OF INFORMATION TECHNOLOGY ASSETS

Article 6. Management of information technology assets

1. Information technology assets include:

a) Information assets such as digital data and information which are processed and stored through the information system;

b) Physical assets such as information technology equipment, means of media, information-bearing objects and equipment that support operation of the information system;

c) Software assets such as software systems, utility software, middleware, database, application programs, source codes and development tools.

2. The institution shall make a list of all information technology assets attached to each information system as prescribed in Clause 3 Article 4 herein. Annual review and update of such list is required.

3. According to the importance of information systems, the institution shall adopt management and protection methods suitable for each type of information technology asset.

4. According to classification of information technology assets prescribed in Clause 1 this Article, the institution shall set up and adopt regulations on asset management and use as prescribed in Article 7, 8, 9, 10 and 11 herein.

Article 7. Management of information assets

1. Each information system requires a list of information assets and regulations on powers and responsibilities of individuals or departments in the institution that are entitled to access to, use and manage such information.

2. Information assets shall be categorized as prescribed in Clause 1 Article 4 herein.

3. Information assets categorized as classified information must be encrypted or secured by appropriate methods for the purpose of information protection during the process of producing, exchanging and storing information.

4. The institution shall employ methods for data leakage prevention applied to information assets contained in Level 3 information systems.

Article 8. Management of physical assets

1. With regard to each information system under management of an institution, such institution shall make a list of physical assets with basic information including name, value, installation position, asset manager, useful purpose, using condition and equivalent information system.

2. Individuals or departments in the institution shall be assigned or bound to take responsibility to use and manage physical assets.

3. Any physical asset moved out of the institution's head office must be approved by the competent person and protected by appropriate methods with the aim of securing the information stored in such asset in case the asset contains classified information.

4. When changing the purpose of use of the physical asset containing classified information or liquidating such asset, the institution shall use methods for completely and permanently eliminating or removing such classified information so that it could not be restored. Where it is impossible to eliminate the classified information, the institution shall adopt a method for eliminating the data storage constituent of such asset.

5. Physical assets that are mobile devices, information-bearing objects and those not prescribed in this Article must be managed as prescribed in Article 10 and 11 herein.

Article 9. Management of software assets

1. As regards each information system, the institution shall make a list of software assets with basic information including name, value, useful purpose, using extent, asset manager, copyright information, version and equivalent information system.

2. Individuals or departments of the institution shall be bound to take charge of management of software assets.

3. Periodic review and update on patches of security-related errors for software assets are required.

4. Software assets shall be stored by information-bearing objects in accordance with regulations in Article 11 herein.

Article 10. Management of mobile devices

1. Mobile devices must be registered for controlling purpose when connecting to the local area network (LAN) of each institution.

2. Mobile devices must be connected to information systems and services of each institution within a limited area and connection from mobile devices to permitted information systems of the institution must be controlled.

3. Regulations on responsibilities of mobile device users in each institution shall be set out.

4. The following technical methods shall be applied to mobile devices for working purpose:

a) Set up the function of remotely disabling and locking the device in case the mobile device is lost or stolen;

b) Back up data on mobile devices to protect and restore data where necessary;

c) Adopt methods for protecting data when mobile devices are sent to warranty, maintenance or repair service providers

5. With regard to mobile devices that are assets of an institution, the following technical methods shall be adopted other than those prescribed in Clause 4 this Article, at least including:

a) Control installed software and update software versions and patches on mobile devices;

b) Install internal and classified information guard software (if any), create a password and install software for prevention of malicious codes and other security-related errors

Article 11. Management of use of information-bearing objects

1. Control connection and disconnection of information-bearing objects from and to devices of the information systems

2. Develop methods to ensure safety of information-bearing objects during the transportation and storage process

3. Adopt methods for protecting classified information contained in information-bearing objects

4. Assign individual responsibilities for management and use of information-bearing objects

Section 2. HUMAN RESOURCE MANAGEMENT

Article 12. Organization of human resources

1. The legal representative of the institution himself/herself must provide guidelines and take responsibility for preparation of strategies and plans for assurance of information security and response to cybersecurity incidents that occur in such institution.

2. Management of Level 2 information systems and above shall be carried out as follows:

a) Establish or assign a department in charge of information security to perform the task of information security assurance and response to cybersecurity incidents for the institution;

b) Establish or appoint a department to manage and operate the center for cyber information security operation meeting requirements specified in Article 46 herein (not applicable to branches of foreign banks, intermediary payment service providers and non-banking credit institutions);

c) People holding the following positions must be separated: (i) Developers and administrators of information systems; (ii) Developers and operators of information systems; (iii) Administrators and operators of information systems; (iv) Information security inspectors, developers, administrators and operators of information systems

Article 13. Recruitment and duty assignment

1. Define responsibilities of each position to which an employee is recruited or assigned for assurance of information security

2. Consider and evaluate personal ethics and professional qualifications based upon curriculum vitae and juridical record of each employee before appointing such employee to vital position of the information system such as operator of Level 3 information system or information system administrator

3. Request the recruited candidates to make a written commitment to information security on a separate basis or give such commitment in the labor contract. Such commitment must include terms and conditions regarding responsibilities for information security during and after a period of time working for the institution

4. Provide training in the institution's regulations on information security to newly-recruited employees

Article 14. Personnel management

1. Broadcast and provide updated regulations on information security to all staff members at least once every year

2. Carry out inspection of compliance with information security regulations of every individual and department affiliated to the institution at least once every year

3. Implement disciplinary measures imposed on any individual or department breeching the information security regulations of the soft law and those issued by the institution

Article 15. Employment termination or change

When an employee in an institution terminates or change employment, such institution shall:

1. determine responsibilities of such employee at the date of employment termination or change

2. request such employee to hand over the information technology assets

3. revoke the right to access to the information system of the employee resigning from his/her job

4. timely change the access right to information system of the employee who changes his/her employment in order to conform to the principle that such right is given adequately for him/her to perform the assigned duty.

5. at least every six months, carry out review, inspection and comparison between personnel management department and department in charge of management of granting and revocation of rights to access to information systems for the purpose of complying with regulations specified in Clause 3 and 4 this Article

6. inform the State Bank of Vietnam (Information Technology Authority) of cases in which individuals working in information technology sector of the institution have been disciplined in forms of dismissal, discharge or legal proceedings on account of violations against information security regulations

Section 3. ASSURANCE OF PHYSICAL AND ENVIRONMENTAL SAFETY FOR LOCATION FOR INSTALLATION OF INFORMATION TECHNOLOGY EQUIPMENT

Article 16. General requirements applied to the location for installation of information technology equipment

1. Build guard fences and entrance and exit gates or develop methods for controlling and restricting unauthorized access risks

2. Employ methods for prevention of explosion or flood risks

3. Areas that require high level of information safety or security, including areas for installation of servers, storage devices, security instruments and communications equipment must be isolated from areas for common use, distribution and cargo handling, and must have working rules and instructions as well as take measures to control persons who enter or leave such areas.

Article 17. Requirements applied to the data center

In addition to conformity with requirements specified in Article 16 herein, the data center must satisfy the following requirements:

1. Security guards must be present at entrances and exits at all time.

2. Entrance and exit door must be firm and fireproof and locked with at least two distinct types of security keys and put under 24/7 surveillance and guard.

3. Areas for equipment installation must be waterproof and protected from direct sunlight as well as floods.

Areas for installation of equipment of Level 2 information systems and above must be put under 24/7 guard and surveillance.

4. There must be at least one power source supplied by the grid and one supplied by the power generator. The automatic transfer switch between two power sources must be available. Whenever power source supplied by the power transmission grid is cut, the power generator must automatically run to supply power. The power source must be connected through UPS system to supply power for equipment and ensure the capability to maintain continuous operations of the information system.

5. There must be an air conditioner system to ensure continuous operations.

6. There must be a lighting protection system and surge protection system.

7. There must be an automatic fire alarm and fire suppression to ensure that firefighting activities do not cause harm to the built-in equipment.

8. There must be a technical floor system or electricity insulating layer and earthing system.

9. There must be a surveillance camera and data storage system which has capacity to store data within 100 days.

10. There must be a temperature and humidity monitoring and controlling system.

11. There must be an entrance and exit logbook.

Article 18. Physical asset security

1. Physical assets must be arranged or installed in a safe and guarded position in order to reduce risks incurred by environmental threats or perils and unauthorized access.

2. Physical assets belonging to Level 2 information systems and above must be provided with an adequate amount of power and support systems whenever interruption of the main power source occurs. Electric overload, voltage sag or surge protection solutions, earthing system, standby generation system and UPS system must be in place to ensure continuous operations.

3. Power supply and communication cables used for data transmission or other information support services must be protected from infringement and damage.

4. Equipment used for professional operations that are installed outside the head office of the institution must be supervised and protected from any act of infringement and unauthorized access.

Section 4. MANAGEMENT OF OPERATION AND INFORMATION EXCHANGE

Article 19. Management responsibilities and operational procedures of the institution

1. The institution shall establish procedures for operation of Level 2 information systems and above which at least including the following contents: system startup and shutdown, data backup and restoration, application operation, troubleshooting and supervision and recording of system operations into a logbook. For the purpose of such procedure, scope and responsibilities of persons who use and operate the systems must be clearly determined. At least once every year, the institution shall carry out necessary review, provide update and amendments to procedures for operation of information systems to satisfy actual conditions.

2. The institution shall introduce procedures to all staff members involved in the operation and supervise the compliance with those issued procedures.

3. Operational environment of Level 2 information systems and above must meet the following requirements:

a) Such environment must be independent from environment of development, inspection and experiment;

b) Measures to ensure information security must be applied;

c) Installation of application development equipment and instruments are not permitted;

d) All functions and utility software that are not currently in use on information systems shall be eliminated or turned off.

4. Information systems for handling client's transaction must satisfy the following requirements:

a) A single individual is not allowed to participate in different processes varying from conduction or ratification of a transaction;

b) Measures to ensure integrity of transaction data must be applied;

c) All activities on the information systems must be tracked and recorded for inspection and control purpose where necessary.

Article 20. Plan preparation and information system acceptance

1. The institution shall develop technical standards, restrictions and requirements to ensure normal operations of all current information systems and other information systems before officially putting those systems in use.

2. According to technical standards, restrictions and requirements which have been developed, the institution shall carry out surveillance and maximization of performance of information systems, and assessment of demand satisfaction, operating condition and system configuration of information systems for the purpose of forecasting and preparing extension and refine plans to ensure the demand satisfaction capability in the future.

3. The institution shall carry out necessary review and provide update on technical standards, restrictions and requirements in case of any change made to information systems, and provide relevant staff members with technical training and technical transfer in terms of elements subject to such change.

Article 21. Data backup

Data shall be backed up to ensure data security as follows:

1. The institution shall make a list of information systems categorized in order of importance that require to be duplicated with storage period, backup time, backup method and time of testing for system restoration from the backup file .

2. Data of Level 2 information systems and above must be automatically backed up in consistent with the frequency of data change in order to adhere to the principle that any newly-generated data must be backed up within 24 hours. Data must be backed up in external storage devices such as magnetic tapes, hard disks, optical tapes or other storage devices and must be retained and stored and separated from the area of information system sources.

3. With regard to Level 2 information systems and above, it is required to check and restore backup data stored in external storage devices at least once every six months.

4. The institution which owns both main and standby information systems set out outside of the Vietnamese territory must store personal information and transaction data of the clients in Vietnam in accordance with provisions of the Vietnam law.

Article 22. Management of network safety and security

Network safety and security shall be managed as follows:

1. Formulate regulations on management of network safety and security and management of terminal devices of the entire information systems

2. Make and store records of logical and physical diagrams relating to the network systems, including wide area network (WAN/Intranet) and local area network (LAN)

3. Develop a computer network system of an institution meeting the following requirements:

a) Network areas must be separated from one another according to the users, purposes of use and information systems, at least including: (i) a separate partition for the server of Level 2 information system and above; (ii) demilitarized zone (DMZ) for Internet services; (iii) independent network for wireless network services.;

b) There must be devices with firewall installation to control connections and access to important network areas;

c) There must be devices with firewall installation and software for detecting, preventing and fighting against unauthorized access to control connections and access from untrusted network to the network system of the institution;

d) Measures to timely control, detect and prevent unauthorized connections and access to the local area network system of the institution which owns Level 2 information systems and above must be applied;

dd) Download balance plans and denial of service attack handling plans applied to Level 2 information systems and above which provides services on the Internet must be prepared;

4. Applications must be developed and configured according to the design of network security equipment; methods for tracing and timely identifying technical vulnerabilities, holes of the network systems must be adopted and regular inspection and detection of illegal connections or installation of equipment and software to the network system must be carried out.

Article 23. Information exchange

The institution shall take the following responsibilities for information exchange with clients and third parties:

1. Issue information exchange regulations including the following contents: type of information exchanged, powers and responsibilities of each individual getting access to information, means of information exchange; methods for ensuring integrity and confidentiality of information during the process of transmitting, receiving and processing and information preservation regime

2. Make a written commitment in which responsibilities and obligations of all parties involved in information use and assurance of information security are clearly defined when exchanging internal and classified information with external parties

3. Employ encryption methods or information security methods applied to classified information before the exchange

4. Use methods for protecting information exchange equipment and software in order to prevent illegal access and utilization

5. Adopt methods for strictly managing, supervising and controlling websites that provide online information, services and transactions to the clients

Article 24. Management of online transaction services

1. Information systems that provide online transaction services for clients must satisfy the following requirements:

a) Ensure integrity of information exchanged with the clients during the online transaction;

b) Ensure confidentiality of information on the transmission line and deliver sufficient information to the right address, and develop protection methods for preventing such information from being corrected or replicated in an illegal manner;

c) Assess potential risks incurred in online transactions according to the clients, type of transaction and transaction limit with the aim of working out feasible solutions for transactions in conformity with regulations of the State Bank of Vietnam;

d) Apply anti-phishing authentication measures and methods for preventing and fighting against illegal alteration to websites which provide online transaction services

2. Clients' transactions shall be authenticated directly on the information system of the institution. In case the authentication service is provided by a third party, such institution must take responsibility to manage at least one authentication factor.

3. Information systems that provide online transaction services must have methods for strict supervision, detection and warning of:

a) suspected transactions based upon determination of transaction time and place (geographical location and IP network), transaction frequency rate, transaction monetary amount and number of authentication inconsistent with regulations;

b) Abnormal operations of the systems;

c) Denial of Service attack (DoS) and Distributed Denial of Service attack (DDoS)

4. The institution shall give instructions for information security assurance methods and warning of risks to clients before use of online transaction services and on a periodic basis.

5. Methods for ensuring software integrity must be employed when online transaction applications and software on the Internet are provided.

Article 25. Supervision and recording of operations of information systems into the logbook

Operations of information systems shall be monitored and recorded into the logbook as follows:

1. Record operations of information systems and users, errors and information insecurity incidents into a logbook and retain such logbook. Data contained in logbooks of Level 2 information systems and above must be preserved online for at least three months in a concentrated manner and backed up at least once a year.

2. Protect the function of logbook recording and information contained in the logbook, anti-phising and unauthorized access and ensure that the system administrators and users could not remove or revise the logbook containing their own activities on the system

3. Synchronize the time of different information systems

Article 26. Malicious code protection

Regulations on malicious code protection shall be made and satisfied as follows:

1. Define responsibilities of individuals and departments relating to protection from malicious codes

2. Employ methods for protecting from malicious codes applied to the entire information systems of the institution

3. Update new malicious code samples and malware protection software

4. Check and remove malicious codes for externally-received information-bearing objects before use

5. Control the software installation to ensure compliance with information security regulations of the institution

6. Take control of unknown emails, enclosures or links attached to unknown emails

Section 5. ACCESS MANAGEMENT

Article 27. Requirements for access management

1. Regulations on access management applied to users, groups of user, equipments and instruments used for accessing to information systems satisfying professional requirements and information security requirements shall include basic contents as follows:

a) Registration, granting, extension and revocation of access rights of the users;

b) Each account getting access to the system must be given to a single user; in case one account is shared by different persons for access purpose, such common use must be approved by competent authorities and responsibilities of each person at each using time must be defined.

c) With regard to Level 2 information systems and above, limit and control access from administrators' accounts: (i) Develop a mechanism to control opening of administrators' accounts with the aim of ensuring that no administrator's account could be put in use without approval of competent authorities; (ii) Work out methods for controlling use of administrators’ accounts; (iii) Administrators' accounts must be used within a time limit which ensures task completion and must be revoked right after such completion.

d) Manage and grant passwords to access to information systems;

dd) Review, check and revise users’ access rights;

Set out information security requirements applied to equipment and instruments used for access purpose

2. Regulations on password management must meet the following requirements:

a) Any password must contain at least six characters including numbers, uppercase lattes, lowercase letters and special characters if allowed by the systems; Valid requests for passwords must be automatically checked when a password is set up;

b) Any default password set by a manufacturer on a device, software and database must be changed before use;

c) Password management software must be developed with the following functions: (i) Requesting for password change in first login (not applicable to one-time passwords); (ii) notifying users of change of an expired password; (iii) invalidating an expired password; (iv) invalidating an password in case the number of incorrect entry exceeds the permitted one; (v) granting permission to promptly change a password which has been disclosed or is exposed to a risk of being disclosed or upon the request of users; (vi) preventing use of old password during a specified period.

3. Regulations on responsibilities of users who are granted access rights shall include the following contents: using passwords in accordance with regulations, ensuring password confidentiality, using equipment or instruments for access purpose and signing out of the systems when stopping work or temporarily leaving the systems.

Article 28. Management of access to the local network

Policies on management of access to the local area network shall be formulated and implemented meeting the following requirements:

1. Issue regulations on management of network access and network services including the following basic contents:

a) Networks and network services permitted for use, mode, means and requirements of information security for access purpose;

b) Responsibilities of administrators and users;

c) Procedures for granting, changing and revoking connection rights;

d) Control of network access, use and administration

2. Employ methods for strict control of connections from untrusted networks to the local area network of the institution for the purpose of information security assurance

3. Take control of installation and use of remote access tools and software

4. Control access to ports used for setting and administration of network devices

5. Grant right to access to a network and network service under the principle that such right is sufficient to perform the assigned tasks

6. Connect through the Internet to the local area network of the institution for the purpose of virtual private network use and multi-factor authentication

Article 29. Management of access to information systems and applications

Access management shall satisfy the following requirements:

1. Take control of utility software possibly affecting information systems

2. Regulate time of application access corresponding with the time of professional operations and services provided by such application Automatically switch off a working session after a rest time in order to prevent unauthorized access

3. Manage and give the right to access to information and applications adhering to the principle that such right is sufficiently granted to perform tasks assigned to the users. To be specific:

a) Give rights to access to each folder and function of each program;

b) Give rights to read, record, remove and use information, data and programs

4. Information systems supported from a common resource must be approved by competent authorities.

5. With regard to servers of Level 2 information systems and above, it is required to establish a secure connection and auto login prevention plan.

Article 30. Management of Internet access

Regulations on management of Internet access shall meet the following requirements:

1. a) Make regulations on management of connection and access to the Internet including the following basic contents:

a) Responsibilities of individuals and departments involved in use of the Internet;

b) Type of persons permitted to connect and access to the Internet;

c) Restricted and prohibited acts;

d) Internet access and connection control;

dd) Information security methods for Internet connection

2. Manage Internet connection ports of the entire institution in a concentrated and consistent manner

3. Provide network security solutions for Internet connection ports with the aim of ensuring security against risks from Internet attacks into the local area network of the institution

4. Use instruments for timely detecting and identifying vulnerabilities, holes, attacks as well as illegal access to the local area network of the institution through Internet connection ports.

Section 6. MANAGEMENT OF USE OF INFORMATION TECHNOLOGY SERVICES PROVIDED BY THIRD PARTIES

Article 31. General principles for use of services provided by third parties

When using information technology services provided by a third party, the institution shall adhere to the following principles:

1. Do not reduce the capacity to provide continuous services for clients of such institution

2. Do not reduce control of professional procedures of such institution

3. Do not change responsibilities for ensuring information security of such institution

4. Information technology services provided by the third party must satisfy regulations on information security issued by such institution

Article 32. Requirements for use of services provided by third parties

Before using services provided by a third party, the institution shall perform the following tasks:

1. Carry out assessment of information technology risks and operating risks which at least includes:

a) Identifying risks, analyzing and estimating the extent of damage and threats to information security;

b) Defining capacity to control professional procedures, capacity to provide continuous services for the clients and capacity to provide information for regulatory agencies;

c) Clearly determining responsibilities for service quality assurance of parties concerned;

d) Working out risk minimizing methods and trouble preventing and solving methods;

dd) Reviewing and adjusting policies on management of risks (if any)

2. If using the cloud computing service, in addition to requirements specified in Clause 1 this Article, the institution shall take on the following duties:

a) Separate activities and professional tasks expected to be performed on cloud computing based upon assessment of impacts of the aforesaid activities and professional tasks on operations of the institution;

b) Prepare backup plans for components of Level 2 information systems and above Backup plans must be tested and assessed to see whether they are available to replace activities and professional tasks performed on the cloud computing;

c) Set out criteria for selection of third parties meeting requirements specified in Article 33 herein;

d) Review, amend and apply information security methods of the institution and limit access through cloud computing to information systems of such institution

3. In case the third party is hired to perform all administration activities for Level 2 information systems and above, the institution shall carry out risk assessment as prescribed in Clause 1 this Article and send reports on such assessment to the State Bank of Vietnam (Information Technology Authority).

Article 33. Criteria for selecting a third party providing the cloud computing service

Any third party shall be selected if it:

1. is an enterprise;

2. owns information technology infrastructure corresponding to the service requested by the institution which:

a) complies with provisions of Vietnamese laws;

b) is granted an unexpired international certificate of information securiry.

Article 34. Contract for service use with a third party

The contract for service use with a third party shall at least contain the following contents:

1. Commitment to ensure information security made by the third party which includes:

a) Meeting requirements specified in Article 33 herein;

b) Not replicating, altering, using or providing data of the institution using the service for another individual or institution, except for cases required by competent regulatory agencies as per law provisions; in such case, the third party is required to notify the institution using the service of data provision to another institution before such provision, unless cases in which notification will go against the law of Vietnam;

c) Broadcasting information security regulations issued by the institution to staff members of the third party involved in contract execution and using monitoring methods for ensuring conformity with the aforesaid regulations

2. Regulations on time limit for service interruption and troubleshooting time, requirements regarding assurance of continuous operation (on-site backup, backup data, disaster recovery), requirements regarding storing, calculating and processing capacity as well as actions taken in case of lack of service quality assurance

3. Cases in which lease of a auxiliary contractor by the third party causes no change in responsibilities of such third party for services in current use of the institution

4. Data generated during the service use that is considered asset of the institution. When the service use is terminated:

a) The third party shall return all data used and data generated during the service use;

b) The third party shall make a commitment to delete all data of the institution within a specified period.

5. Notification of any violations against information security regulations applied to the service in use committed by staff members of the third party

6. The contract for use of cloud computing service containing the following additional contents apart from those prescribed in Clause 1, 2, 3, 4 and 5 this Article:

a) The third party must provide reports on audit of compliance with information technology regulations conducted by independent audit authority every year within the time of contract execution;

b) The third party must provide instruments for control of cloud service quality and procedures for monitoring and control of cloud service quality;

c) The third party must clearly designate locations (cities or countries) for establishment of the data center outside of the Vietnamese territory which provides services for the institution;

d) Responsibilities for data protection and prevention of unauthorized access to data through service distribution channels from the third party to institution must be defined;

dd) The third party must assist and cooperate in investigation carried out as required by competent regulatory agencies of Vietnam as per law provisions;

e) Data of the institution must be separated from other clients' data used on the same technical basis provided by the third party.

Article 35. Responsibilities of the institution during the use of services provided by a third party

1. Provide, notify and ask the third party to comply with information security regulations issued by the institution.

2. Establish procedures and allocate resources to monitor and control services provided by the third party with the aim of ensuing service quality under provisions of the signed contract. With regard to cloud computing services, monitoring and control of service quality are required.

3. Impose the institution's information security regulations on devices and services provided by the third party which are operated on the infrastructure used and managed by such institution.

4. Manage changes in services provided by the third party including changes made to suppliers, solutions, versions and changes of contents specified in Article 40 herein and assess all impacts of those changes for safety assurance before use

5. Employ methods to strictly monitor and limit access right of the third party when such party is allowed to obtain access to information systems of the institution.

6. Supervise staff members of the third party during the contract execution. If discovering any violation against information security regulations committed by such staff member, the institution shall notify and cooperate with the third party in timely handling.

7. Revoke right to access to information systems granted to the third party, change locks and passwords transferred from such third party right after job completion or contract termination.

8. With regard to Level 2 information systems and above or information systems using cloud computing services, assessment of compliance with information security regulations of the third party under provisions of the signed contract must be carried out. Carry out annual or irregular assessment of compliance with regulations as required. Results of information technology audit conducted by the independent audit authority may be used in such assessment.

Section 7. MANAGEMENT OF ACCEPTANCE, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

Article 36. Requirements for information system safety and security

When creating or improving its information systems, the institution must classify information systems in order of importance as prescribed in Clause 2 Article 4 herein. With regard to Level 2 information systems and above, such institution shall take on the following obligations:

1. Prepare design data and description of information security plans. For the purpose of such data and description, safety and security requirements shall be set out in conjunction with technical and professional requirements.

2. Prepare system testing and verifying plans which is launched in consistent with the design data meeting information security requirements before acceptance. The testing results must be reported in writing and approved by competent authorities before use.

3. Strictly monitor and manage purchase of external software in compliance with regulations in Article 35 herein

Article 37. Assurance of safety and security for applications

Application programs supporting operations of the institution must at least satisfy the following requirements:

1. Verify validity of data input into applications and ensure the input data is accurate and valid

2. Verify validity of data requiring automatic processing contained in applications for the purpose of detecting false information incurred by processing errors or intentional information alteration

3. Work out methods for ensuring authenticity and protecting integrity of data processed by applications

4. Verify validity of data retrieved from applications and ensure information is processed by applications in an accurate and valid manner

5. Users' passwords in Level 2 information systems and above must be encrypted at the application layer.

Article 38. Encryption management

Encryption shall be managed as follows:

1. Develop and employ encryption methods under national technical regulations on data encryption applied to banking or accredited international standards

2. Work out encryption management methods in order to protect information of the institution

Article 39. Safety and security for software development

1. The institution shall manage software development as follows:

a) Manage and control source programs

Any access or approach to source programs must be approved by the competent authority;

b) Manage and protect system configuration folders

2. Select and control testing and experiment data Real data of information systems in current operation is not allowed to be used in testing activities if the data containing client's information and classified information are not changed or hidden.

Article 40. Management of changes in information systems

The institution shall issue procedures and methods for management and control of information system changes which at least include:

1. Recording changes, preparing changing plans, conducting inspection and experiment of changes and making result reports, approving changing plans before making official changes to software version, hardware configuration, software parameters and operational procedures.

Preparing backup plans for system recovery in case of unsuccessful changes or unexpected problems.

2. Carrying out inspection and assessment of effects caused by changes to ensure normal and safe operations in new environment of Level 2 information systems and above in cases of changes made to the version or operating system, database and middleware.

Article 41. Assessment of information system safety and security

1. Assessment of information system safety and security must include the following contents:

a) Assessing system architecture for the purpose of determining conformity of the installed devices to general system architecture and security requirements;

b) Checking configuration of security devices, systems for automatic grant of access rights, systems for management of terminal devices and list of user accounts;

c) Conducting penetration test required for information systems which have connection to and provide information and services on the Internet or connect to clients and third parties

2. The institution shall carry out assessment of security of Level 2 information systems and above as per regulations in Clause 1 this Article before use

3. During operation of information systems, the institution shall carry out security assessment as follows:

a) Carry out assessment once every six months for Level 3 information systems as prescribed in Clause 1 this Article;

b) Carry out assessment once every year for Level 2 information systems and devices directly interacting with the external environment such as connecting to the Internet, clients and third parties as prescribed in Clause 1 this Article;

Carry out assessment once every two years for Level 1 information systems

4. Assessment results must be reported in writing to the legal representative of the institution and the competent authority. As for any content fails to comply with information security regulations (if any), methods, plans and time limit for resolution must be recommended.

Article 42. Management of technical vulnerabilities

The institution shall manage technical vulnerabilities as follows:

1. Set out regulations on assessment, management and control of technical vulnerabilities of active information systems

2. Proactively identify technical vulnerabilities through the following activities:

a) Regularly update information concerning technical vulnerabilities and holes;

b) Carry out scanning and detection of malicious codes, technical holes and vulnerabilities of active information systems at least once every three months in respect of Level 3 information systems having connection to the Internet, and at least once every six months in respect of other information systems.

3. Assess the level of impact and risks caused by technical holes and vulnerabilities of active information systems which have been detected and recommend possible solving plans

4. Develop and adopt troubleshooting methods and report the troubleshooting results

Article 43. Management of information system maintenance

The institution shall carry out information system maintenance as follows:

1. Issue regulations on information system maintenance right after such system is officially put in use Maintenance procedures shall at least contain the following contents:

a) Maintenance scope and subjects;

b) Maintenance time and frequency;

c) Technical scenario and procedures for maintenance of each component and the entire information system;

d) Reports sent to the competent authority for handling purpose if any incident is found during the maintenance;

dd) Duties and responsibilities assigned to department in charge of maintenance and maintenance supervision

2. Carry out maintenance as prescribed in Clause 1 this Article in respect of information systems under management of the institution

3. Review maintenance regulations at least once every year or in case of changes made to information systems

Section 8. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Article 44. Procedures for handling incidents

Incidents shall be managed as follows:

1. Issue procedures for handling information security incidents including the following contents:

a) Receiving any information on incidents incurred;

b) Assessing the level and extent of impacts of such incident on operations of information systems. According to the level and extent of the incident, the institution shall report such incident to equivalent level of management authorities for guidelines on troubleshooting

c) Employing troubleshooting methods;

d) Recording and reporting the troubleshooting results

2. Assign responsibilities to individuals and collectives in terms of reporting, receiving and handling information security incidents

3. Create forms for recording and storing troubleshooting documents

Article 45. Incident handling and control

Incidents shall be controlled and handled as follows:

1. Make a list of information security incident and troubleshooting plan in respect of Level 2 information systems and above and review and update such list and plan at least once every six months

2. Immediately report to the competent authority and relevant persons if any information security incident is found for the purpose of finding solutions as soon as practicable

3. Collect, record, protect and store evidence at the institution during incident inspection and handling

4. Assess and determine causes, and adopt methods for prevention of incident recurrence after troubleshooting

5. In case information security incidents relate to violations against laws, the institution shall take responsibility to collect and provide evidence for competent authorities in accordance with law soft provisions.

Article 46. Network Security Operation Center

The Network Security Operation Center shall take on the following obligations:

1. Proactively monitor, collect and receive any information and warning about internal and external information security risks.

2. Develop a system for security information and event management, collect and store information in a concentrated manner, at least including: logbooks of Level 2 information systems and above and warning and logbook of network security equipment such as firewall and IPS/IDS.

3. Analyze information in order to detect and warn in respect of cyberattack risks and threats and cybersecurity incidents and send reports to the system administrator if finding any incident relating to 24/7 information systems for client services, online transaction information systems and Level 3 information systems.

4. Coordinate incident response activities, zone, prevent and minimize impact and damage to information systems if any incident occurs.

5. Carry out investigation and determination of attack methods, modes and causes and take measures to prevent incident recurrence.

6. Provide information as required by the State Bank for the purpose of network security surveillance in baking

Article 47. Cybersecurity incident response activities

1. Cybersecurity incident response team in banking (hereinafter referred to as “the team”) shall cooperate with internal and external resources in efficient cybersecurity incident response which helps to ensure safety in banking operations.

2. The team shall include:

a) The Steering Committee established by the State Bank’s Governor;

b) Coordinating authority which is the Information Technology Authority (State Bank);

c) Members of the team: the Information Technology Authority (State Bank), credit institutions (departments in charge of information security) and voluntary members which may be voluntary organizations or business facilities

3. Principles for incident response and coordination

a) Organizations prescribed in point c Clause 2 this Article shall take responsibility to provide resources and become members of the team;

b) If any cybersecurity incident is found, the members must notify such incident to the coordinating authority as prescribed in Clause 1 Article 53 herein;

c) If facing serious incidents which could not be handled on their own, the members shall request help from the coordinating authority;

d) According to each incident, the coordinating authority shall ask for assistance of the members or competent regulatory agencies.

4. Principles for information management and use in incident response and coordination:

a) Information exchanged and provided during incident response and coordination must be classified information;

b) Any act of use of information exchanged during incident response and coordination which cause negative effects on prestige and image of the organization proving such information is prohibited.

Section 9. ASSURANCE OF CONTINUOUS OPERATION OF INFORMATION SYSTEMS

Article 48. Principles for continuous operation assurance

1. The institution shall at least satisfy the following requirements:

a) Analyze impact and assess risks in respect of interruption or termination of information system operation;

b) Establish a scenario and procedure for assurance of continuous operation of information systems as prescribed in Article 50 herein;

c) Adopt methods for ensuring continuous operation as prescribed in Article 51 herein.

2. Based upon impact analysis and risk assessment specified point a Clause 1 this Article, the institution shall make a list of information systems requiring continuous operation assurance, at least including:

a) Information systems supporting daily internal activities of the institution without operation termination over 4 working hours;

b) 24/7 information systems for client services;

c) Information systems providing online transaction services for clients;

d) Level 3 information systems 0}

3. Information systems requiring continuous operation assurance specified in Clause 2 this Article must ensure great availability and have disaster recovery systems.

Article 49. Establishment of disaster recovery systems

1. The institution shall establish a disaster recovery system meeting the following requirements:

a) It is required to carry out risk assessment and consider possibility of disasters having impact on both main information system and disaster recovery system when selecting the location for establishment of the disaster recovery system such as natural disaster including earthquake, flood and widespread epidemic, disasters caused by human and technologies including power network incidents, fire, traffic incidents and cybersecurity attacks;

b) Location for establishment of the disaster recovery system must satisfy requirements specified in Article 16 herein;

c) The disaster recovery system must be capable to replace the main system within 4 hours in respect of the information system supporting daily internal activities of the institution without operation termination over 4 working hours, 24/7 information system for client services, information system providing online transaction to the clients and Level 3 information system, and within 24 hours with regard to other systems.

2. Institutions that only have a single office in Vietnam must have a standby office which is located in a different area and separated from the main office, and equipped with necessary devices to ensure continuous operation of information systems instead of the main one.

Article 50. Formulation of procedures and scenario for assurance of continuous operation of information systems

The procedure and scenario for assurance of continuous operation shall be established as follows:

1. Establish a procedure for response to operational insecurities and interruptions of each component of Level 2 information systems and above

2. Construct a scenario for conversion of operation from the main system to the standby one, including job description, conversion process and expected completion date which meet the following requirements:

a) Have necessary resources, instruments and conditions for conversion;

b) Have forms for result recording;

c) Assign staff members involved in the conversion to give instructions for conversion, monitor, carry out conversion, operate the system and check the results;

d) Take measures to ensure information security;

dd) Prepare plans for assurance of continuous operation in case of unsuccessful conversion

3. The institution that has a single office in Vietnam must construct a scenario for conversion of its operation to the standby office.

4. Conversion procedures and scenario must be checked and updated in case of changes made to information systems, organizations structure, personnel and responsibilities given to relevant departments in the institution

Article 51. Implementation of plans for continuous operation assurance

1. Plans for assurance of continuous operation of information systems shall be prepared and implemented meeting the following requirements:

a) Carry out inspection and assessment of operation of the standby system at least once every six months;

b) Carry out annual conversion of operation from the main system to the standby one within at least 1 working day of each information systems according to the list provided in Clause 2 Article 48 herein and assess the conversion results as well as provide update on conversion procedures and scenario (if any)

2. Institutions that have a single office in Vietnam must perform annual drill for operational conversion to ensure continuous operation of information systems.

3. Plans for operational conversion drill shall be notified to the State Bank (Information Technology Authority) within 5 working days before such drill.

Section 10. INTERNAL INSPECTION AND REPORTING MECHANISM

Article 52. Internal inspection

The institution shall carry out internal inspection as follows:

1. Set out regulations on internal inspection in respect of information security assurance

2. Prepare plans and carry out internal inspection of compliance with regulations herein and internal regulations on information security assurance at least once every year

3. Send reports on results of information security inspection to the legal representative of the institution and competent authorities in which plans for dealing with problems failing to comply with information security regulations (if any) that remain unsolved shall be provided

4. Implement such plan and report the results of handling of unsolved problems stated in the aforesaid reports as prescribed in Clause 3 this Article

Article 53. Reporting mechanism

The institution shall send reports to the State Bank (Information Technology Authority) including the following contents:

1. Reports on cybersecurity incidents sent within 24 hours starting from the detection of such incident and within 5 working days after incident handling under instructions provided in the Appendix issued thereto to the email address antt@sbv.gov.vn.

2. Reports on risk assessment as prescribed in Clause 3 Article 32 herein sent directly or by post to the State Bank (Information Technology Authority, 64 Nguyen Chi Thanh, Hanoi City) in

case all management activities for Level 2 information systems and above of the institution are performed by another organization under a lease contract, which is sent 10 working days before such management

Chapter III

IMPLEMENTATION PROVISIONS

Article 54. Responsibilities of entities affiliated to the State Bank

1. The Information Technology Authority shall take responsibility to:

a) monitor and send consolidated reports on implementation of institutions to the Governor of the State Bank as per regulations herein;

b) prepare annual plans for inspection of implementation of this Circular;

c) preside over and cooperate with relevant entities affiliated to the State Bank in dealing with questions arising during implementation of this Circular

2. Banking monitoring and inspection authorities shall cooperate with the Information Technology Authority in carrying out inspection of implementation of this Circular at each institution and handling administrative violations in accordance with law provisions.

Article 55. Effect and implementation

1. This Circular comes into effect from January 01, 2019 unless otherwise prescribed in Clause 2 this Article and replaces Circular No.31/2015/TT-NHNN dated December 28, 2015 of the State Bank's Governor on assurance of safety and security for information technology systems in banking operation and Decision No.29/2008/QD-NHNN dated October 13, 2008 of the State Bank’s Governor which promulgates regulations on maintenance of informatics equipment systems in banking.

2. Point b Clause 2 Article 12 comes into force from January 01, 2020.

3. Director of the Information Technology Authority, Directors of relevant entities affiliated to the State Bank, Chairman of Boards of Director, Member Councils, Directors General (Directors) of credit institutions, branches of foreign banks and intermediary payment service providers shall take responsibility to implement this Circular ./.

PP. GOVERNOR
DEPUTY GOVERNOR

Nguyen Kim Anh